Acta Sci. Math., 50 (1986), 287—298

Rédei-Funktionen und ihre Anwendung in der Kryptographie

RUPERT NÖBAUER[1])

1. Einleitung. In [8] hat L. RÉDEI eine Klasse von rationalen Funktionen über einem endlichen Körper K ungerader Ordnung untersucht, die Permutationen von K induzieren.

In der vorliegenden Arbeit erfolgt nun u.a. eine Übertragung der von L. Rédei gefundenen Ergebnisse von endlichen Körpern K auf Restklassenringe $Z/(m)$ des Rings der ganzen rationalen Zahlen modulo ungerader natürlicher Zahlen m. In Abschnitt 2 werden rationale Funktionen über $Z/(m)$ definiert, die den von L. Rédei untersuchten Funktionen entsprechen und die daher als Rédei-Funktionen bezeichnet werden. Es wird gezeigt, daß bestimmte Mengen von Permutationen von $Z/(m)$, die durch solche Rédei-Funktionen induziert werden, bezüglich der Komposition Gruppen bilden. In Abschnitt 3 wird die Anzahl der Fixpunkte der durch Rédei-Funktionen induzierten Permutationen von $Z/(m)$ berechnet. In Abschnitt 4 wird die Struktur von durch Rédei-Funktionen induzierten Permutationsgruppen von $Z/(m)$ ermittelt, und es werden alle ungeraden m bestimmt, für die diese Gruppen zyklisch sind. In Abschnitt 5 wird u.a. gezeigt, daß es für jedes ungerade $m \geqq 3$ Permutationen von $Z/(m)$ gibt, die durch Rédei-Funktionen induziert werden und die nur *einen* Fixpunkt aufweisen, und es wird eine Aussage über die Anzahl derartiger Permutationen hergeleitet.

In Abschnitt 6 erfolgt die Beschreibung eines Public-Key Kryptosystems — also eines Verschlüsselungssystems mit öffentlich bekanntem Schlüssel (vgl. [1]) — auf der Basis von Rédei-Funktionen. Das Verfahren kann als Variante des RSA-Schemas (siehe etwa [9]) angesehen werden: Beim RSA-Schema erfolgt die Verschlüsselung der Nachrichten mit Hilfe solcher Permutationen von $Z/(m)$, die durch Potenzen x^n induziert werden, beim vorliegenden System erfolgt sie mit Hilfe von durch

Received March 21, 1984 and in revised form July 17, 1984.

[1]) Der Autor dankt dem Institut für Mathematik der Universität Klagenfurt für die Ermöglichung dieser Arbeit. Weiters dankt der Autor dem Referenten für wertvolle Verbesserungsvorschläge.

Rédei-Funktionen induzierten Permutationen. Das vorliegende System ist eine Verallgemeinerung des von R. LIDL und W. B. MÜLLER in [3] vorgeschlagenen Systems, und zwar von $Z/(m)$, m quadratfrei, auf $Z/(m)$, m beliebig.

2. Einige grundlegende Tatsachen. Wir wollen zunächst einige allgemeine Bemerkungen über rationale Funktionen machen, die Permutationen von $Z/(m)$ induzieren. Sei m eine beliebige natürliche Zahl und sei $f(x)=g(x)/h(x)$ Quotient von ganzzahligen Polynomen, welche teilerfremd in $Z[x]$ sind. Man nennt $f(x)$ Permutationsfunktion von $Z/(m)$, wenn $h(u)$ für jedes ganze u eine prime Restklasse mod m ist und wenn die Abbildung $\pi: u \to g(u)h(u)^{-1} \bmod m$ von $Z/(m)$ in sich eine Permutation ist (vgl. [6]). Ist speziell $h(x)=1$ und $f(x)=g(x)/1$ eine Permutationsfunktion von $Z/(m)$, so nennt man $f(x)$ Permutationspolynom von $Z/(m)$. Ist $m=ab$ mit[2] $(a,b)=1$, so ist $f(x)$ genau dann Permutationsfunktion von $Z/(ab)$, wenn es Permutationsfunktion von $Z/(a)$ und von $Z/(b)$ ist. Weiters ist $f(x)$ genau dann Permutationsfunktion von $Z/(p^e)$, $e>1$, wenn gilt: $f(x)$ ist Permutationsfunktion von $Z/(p)$, und $f'(u)\not\equiv 0 \bmod p$ für jedes ganze u (vgl. [6]).

Man nennt zwei Permutationsfunktionen $f_1(x)$, $f_2(x)$ von $Z/(m)$ äquivalent, wenn es ein lineares Polynom $p(x)=cx+d$, $(c,m)=1$, gibt, sodaß gilt

$$f_2(x) = p^{-1}(x) \circ f_1(x) \circ p(x),$$

wobei $p^{-1}(x)$ das bezüglich der Komposition $\circ$ zu $p(x)$ inverse Polynom $c^{-1}x-c^{-1}d$ bezeichnet.

Sei n eine ungerade natürliche Zahl, und sei α eine ganze Zahl mit α Nichtquadratelement in Z, also mit α Nichtquadratelement in Q, dem Körper der rationalen Zahlen. Seien $g_n(x)$, $h_n(x) \in Z[x]$ definiert durch

$$(x+\sqrt{\alpha})^n = g_n(x)+h_n(x)\sqrt{\alpha}. \tag{2.1}$$

Eine explizite Darstellung von $g_n(x)$ und $h_n(x)$ ist gegeben durch[3]

$$g_n(x) = \sum_{i=0}^{[n/2]} \binom{n}{2i} \alpha^i x^{n-2i}, \quad h_n(x) = \sum_{i=0}^{[n/2]} \binom{n}{2i+1} \alpha^i x^{n-2i-1}.$$

Es gilt $h_n(x)\neq 0$ in $Q(\sqrt{\alpha})(x)$, dem rationalen Funktionenkörper über $Q(\sqrt{\alpha})$, und somit $h_n(x)\neq 0$ in $Z[x]$. Denn wäre $h_n(x)=0$, so würde folgen $(x+\sqrt{\alpha})^n = g_n(x)$, also $(\sqrt{\alpha})^n \in Z$, und dies ergäbe einen Widerspruch.

Die Polynome $g_n(x)$, $h_n(x)$ sind teilerfremd in $Z[x]$, denn für $d_n=(g_n(x), h_n(x))$ erhält man aus (2.1) durch Herausheben von $d_n(x)$ unter Beachtung der Tatsache,

[2] $(a_1, \ldots, a_n)$ bezeichne den größten gemeinsamen Teiler, $[a_1, \ldots, a_n]$ das kleinste gemeinsame Vielfache der Zahlen $a_1, \ldots, a_n$.

[3] $[a]$ bezeichne die nächstkleinere ganze Zahl von a.

daß $Q(\sqrt{\alpha})[x]$ ein ZPE-Ring ist: $d_n(x)=(x+\sqrt{\alpha})^s$ mit $0\leqq s<n$. Daraus ergibt sich $s=0$, also $d_n(x)=1$.

Wir setzen nun $f_n(x)=g_n(x)/h_n(x)$. Nach den obigen beiden Bemerkungen ist der Nenner $h_n(x)$ der rationalen Funktion $f_n(x)$ von 0 verschieden, und die Darstellung $g_n(x)/h_n(x)$ ist bereits gekürzt. In $Q(\sqrt{\alpha})(x)$ gilt

$$\left(\frac{x+\sqrt{\alpha}}{x-\sqrt{\alpha}}\right)^n = \frac{f_n(x)+\sqrt{\alpha}}{f_n(x)-\sqrt{\alpha}}. \tag{2.2}$$

Daraus folgt

$$\frac{f_{kn}(x)+\sqrt{\alpha}}{f_{kn}(x)-\sqrt{\alpha}} = \frac{f_k(f_n(x))+\sqrt{\alpha}}{f_k(f_n(x))-\sqrt{\alpha}},$$

und man erhält

$$f_k(x)\circ f_n(x) = f_{kn}(x) \tag{2.3}$$

für beliebige natürliche Zahlen k und n.

Für eine ungerade Zahl $m=p_1^{e_1}\ldots p_r^{e_r}$ soll die Menge aller Permutationen von $Z/(m)$ untersucht werden, die durch bestimmte Permutationsfunktionen $f_n(x)$ induziert werden. Daher wird als erstes nach Bedingungen gefragt, under denen $f_n(x)$ Permutationsfunktion von $Z/(m)$ ist.

Es sei $m=p^e$ (p ungerade Primzahl, $e\geqq 1$), α ein quadratischer Nichtrest mod p und n eine natürliche Zahl mit $(n, p^{e-1}(p+1))=1$, dann ist $f_n(x)$ Permutationsfunktion von $Z/(p^e)$. Für $e=1$ folgt dies aus der Arbeit von L. Rédei [8]. Für $e>1$ erhält man aus (2.2) durch beiderseitiges Differenzieren

$$n\left(\frac{x+\sqrt{\alpha}}{x-\sqrt{\alpha}}\right)^{n-1}\frac{-2\sqrt{\alpha}}{(x-\sqrt{\alpha})^2} = \frac{-2f_n'(x)\sqrt{\alpha}}{(f_n(x)-\sqrt{\alpha})^2},$$

also

$$f_n'(x) = \frac{n(x+\sqrt{\alpha})^{n-1}(f_n(x)-\sqrt{\alpha})^2}{(x-\sqrt{\alpha})^{n+1}} =$$

$$= \frac{n(x^2-\alpha)^{n-1}(f_n(x)-\sqrt{\alpha})^2}{(x-\sqrt{\alpha})^{2n}} = \frac{n(x^2-\alpha)^{n-1}(f_n(x)-\sqrt{\alpha})^2}{(g_n(x)-h_n(x)\sqrt{\alpha})^2} = \frac{n(x^2-\alpha)^{n-1}}{h_n(x)^2},$$

und daraus folgt $f_n'(u)\not\equiv 0 \mod p$ für alle ganzen u. Wir nennen derartige Permutationsfunktionen Rédei-Funktionen. Es sei P_{p^e} die Menge aller jener Permutationen von $Z/(p^e)$, die durch Rédei-Funktionen mit einem festen α induziert werden. Wegen (2.3) bildet P_{p^e} bezüglich der Komposition eine Halbgruppe, die als Unterhalbgruppe der vollen Permutationsgruppe von $Z/(p^e)$ regulär und endlich, also sogar eine Gruppe ist. (Im Spezialfall $e=1$ folgt dies ebenfalls aus [8]).

Betrachtet man den allgemeinen Fall $m=p_1^{e_1}\ldots p_r^{e_r}$, so folgt aus dem Vorherigen, daß $f_n(x)$ eine Permutationsfunktion von $Z/(m)$ ist, wenn $(n, p_i^{e_i-1}(p_i+1))=1$ gilt und α ein quadratischer Nichtrest mod p_i, $i=1, \ldots, r$, ist. Ist P_m die Menge aller durch Rédei-Funktionen mit gegebenem α induzierten Permutationen von $Z/(m)$, dann bildet — wiederum wegen (2.3) — P_m eine kommutative Halbgruppe, die regulär und endlich, also sogar eine Gruppe ist.

Die Struktur dieser Gruppe ist unabhängig von der speziellen Wahl von α: Ersetzt man α durch $\alpha\beta^2$, $\beta\not\equiv 0 \bmod p_i$, $i=1, \ldots, r$, so gehen die Permutationsfunktionen $f_n(x)$ über in die äquivalenten Permutationsfunktionen $\beta f_n(x/\beta)$, wie man mit Hilfe von Gleichung (2.1) leicht erkennt. Bezeichnet τ die durch βx induzierte Permutation von $Z/(m)$, so geht also P_m über in die isomorphe Gruppe $\tau P_m \tau^{-1}$.

Die Klärung der Struktur der Gruppe P_m wird in Abschnitt 4 vorgenommen; dabei wird als wesentliches Hilfsresultat die in Abschnitt 3 berechnete Anzahl der Fixpunkte von Permutationen $\pi_n \in P_m$ herangezogen.

3. Fixpunkte. Zur Berechnung der Fixpunktanzahl von Permutationen $\pi_n \in P_m$ werden Kenntnisse über einen speziellen Erweiterungsring von $Z/(p^e)$ benötigt. Sei p eine ungerade Primzahl, sei α eine ganze Zahl mit α quadratischer Nichtrest mod p, und sei $e\geqq 1$. Man bilde den Faktorring $Z[x]/(x^2-\alpha, p^e)$ des Polynomrings $Z[x]$. Da

$$u(x)(x^2-\alpha)+v(x)p^e = a \quad \text{mit} \quad a\in Z$$

dann und nur dann gilt, wenn $a\equiv 0 \bmod p^e$, ist durch

$$\eta(a \bmod p^e) = a \bmod (x^2-\alpha, p^e)$$

ein Monomorphismus von $Z/(p^e)$ in $Z[x]/(x^2-\alpha, p^e)$ definiert, also kann man $Z/(p^e)$ in $Z[x]/(x^2-\alpha, p^e)$ einbetten. Bezeichnet man die Restklasse von x mit $\sqrt{\alpha}$, dann gilt $(\sqrt{\alpha})^2=\alpha$. Somit läßt sich jedes Element von $Z[x]/(x^2-\alpha, p^e)$ darstellen in der Form $a\sqrt{\alpha}+b$ mit $a, b\in Z/(p^e)$. Da aus

$$ax+b = u(x)(x^2-\alpha)+v(x)p^e$$

folgt $a\equiv b\equiv 0 \bmod p^e$, ist diese Darstellung eindeutig. Wir setzen im folgenden $Z(p^e, \alpha)=Z[x]/(x^2-\alpha, p^e)$.

Es gilt: Ist ξ der kanonische Epimorphismus von $Z/(p^e)$ auf $Z/(p)$, so ist durch $\delta(a\sqrt{\alpha}+b)=(\xi a)\sqrt{\alpha}+\xi b$ ein Epimorphismus von $Z(p^e, \alpha)$ auf $Z(p, \alpha)$ definiert, der ebenfalls als der kanonische Epimorphismus bezeichnet werden soll. Wir zeigen nun

Lemma 1. *Die invertierbaren Elemente von $Z(p^e, \alpha)$ sind genau die Elemente $a\sqrt{\alpha}+b$, für die nicht gleichzeitig $a\equiv 0 \bmod p$ und $b\equiv 0 \bmod p$ gilt.*

Beweis. Ist $\beta\in Z(p^e, \alpha)$ invertierbar, dann ist auch $\delta\beta\in Z(p, \alpha)$ invertierbar, also gilt nicht gleichzeitig $a\equiv 0 \bmod p$ und $b\equiv 0 \bmod p$. Gilt umgekehrt nicht

gleichzeitig $a \equiv 0 \mod p$ und $b \equiv 0 \mod p$, dann gilt wegen der Wahl von α

$$\begin{vmatrix} b & a \\ \alpha a & b \end{vmatrix} = b^2 - \alpha a^2 \not\equiv 0 \mod p,$$

also ist die Matrix $\begin{pmatrix} b & a \\ \alpha a & b \end{pmatrix}$ über $Z/(p^e)$ invertierbar, also ist das lineare Gleichungssystem

$$bu + av \equiv 0 \mod p^e,$$
$$\alpha au + bv \equiv 1 \mod p^e$$

lösbar, und für die Lösung des Systems gilt $(a\sqrt{\alpha}+b)(u\sqrt{\alpha}+v)=1$. Somit ist $a\sqrt{\alpha}+b$ invertierbar.

Es werde im folgenden mit G_{p^e} die Gruppe der invertierbaren Elemente von $Z(p^e, \alpha)$ bezeichnet. Wegen Lemma 1 gilt $|G_{p^e}| = (p^e)^2 - (p^{e-1})^2 = (p^{e-1})^2(p^2-1)$. In G_{p^e} bilden die invertierbaren Elemente von $Z/(p^e)$ eine Untergruppe Z_{p^e} der Ordnung $p^{e-1}(p-1)$. Somit gilt $|G_{p^e}/Z_{p^e}| = p^{e-1}(p+1)$.

Klarerweise ist δ ein Epimorphismus von G_{p^e} auf G_p. Grundlegend für das folgende ist

Lemma 2. *Die Gruppe G_{p^e}/Z_{p^e} ist zyklisch.*

Beweis. Da $Z(p, \alpha)$ ein Körper ist, ist G_p zyklisch. Daher ist auch G_p/Z_p zyklisch. Sei gZ_p erzeugendes Element von G_p/Z_p und sei β ein Urbild von g bei δ. Sei o die Ordnung von βZ_{p^e}, dann gilt $\beta^o \in Z_{p^e}$. Es folgt $g^o \in Z_p$, also $o = (p+1)r$. Die Ordnung des Elements $(\beta Z_{p^e})^r = \beta^r Z_{p^e}$ beträgt somit $p+1$, und wir haben gezeigt: In G_{p^e}/Z_{p^e} gibt es ein Element der Ordnung $p+1$.

Wir betrachten nun das Element $\gamma = (1+p\sqrt{\alpha}) \in Z(p^e, \alpha)$. Es gilt $\gamma^{p^0} = 1 + p^1\sqrt{\alpha} + p^2 r_0$ mit $r_0 \in Z(p^e, \alpha)$. Es sei für ein i mit $0 \leqq i < e-1$ schon gezeigt, daß

$$\gamma^{p^i} = 1 + p^{i+1}\sqrt{\alpha} + p^{i+2} r_i \quad \text{mit} \quad r_i \in Z(p^e, \alpha).$$

Dann gilt

$$\gamma^{p^{i+1}} = (\gamma^{p^i})^p = (1 + p^{i+1}\sqrt{\alpha})^p + p^{i+3} s_i = 1 + p^{i+2}\sqrt{\alpha} + p^{i+3} r_{i+1}.$$

Daraus folgt, daß die Ordnung von γZ_{p^e} den Wert p^{e-1} hat, und damit haben wir gezeigt: In G_{p^e}/Z_{p^e} gibt es ein Element der Ordnung p^{e-1}.

In abelschen Gruppen gilt: Haben zwei Elemente x_1, x_2 die teilerfremden Ordnungen o_1 und o_2, dann hat das Element $x_1 x_2$ die Ordnung $o_1 o_2$. Somit hat in G_{p^e}/Z_{p^e} das Element $\gamma\beta^r Z_{p^e}$ die Ordnung $p^{e-1}(p+1)$, und Lemma 2 ist bewiesen.

Lemma 3. *In der Gruppe G_{p^e}/Z_{p^e} bilden die Elemente $(r\sqrt{\alpha}+s)Z_{p^e}$ mit $r \equiv 0 \mod p$ eine zyklische Untergruppe der Ordnung p^{e-1}.*

Beweis. Die Menge der $r\sqrt{\alpha}+s\in G_{p^e}$ mit $r\equiv 0 \bmod p$ ist die Urbildmenge von Z_p bei δ, also selbst eine Untergruppe $U_{p^e}\subset G_{p^e}$ mit $Z_{p^e}\subset U_{p^e}$. Somit ist U_{p^e}/Z_{p^e} Untergruppe von G_{p^e}/Z_{p^e}, die als Untergruppe einer zyklischen Gruppe zyklisch ist. Wegen $|U_{p^e}|=p^{e-1}(p-1)p^{e-1}$ folgt $|U_{p^e}/Z_{p^e}|=p^{e-1}$, womit Lemma 3 bewiesen ist.

Es soll nun die Anzahl der Fixpunkte der durch $f_n(x)$, $(n, p^{e-1}(p+1))=1$, induzierten Permutationen π_n von $Z/(p^e)$ bestimmt werden. Dazu zunächst eine Vorbemerkung: In $Q(\sqrt{\alpha})[x]$ bildet $Z[\sqrt{\alpha}][x]$ einen Unterring; es sei ϱ der kanonische Epimorphismus von $Z[\sqrt{\alpha}][x]$ auf $Z(p^e, \alpha)[x]$. Dann erkennt man durch Anwendung von ϱ auf (2.1), daß

$$(x+\sqrt{\alpha})^n = g_n(x)+h_n(x)\sqrt{\alpha}$$

auch in $Z(p^e, \alpha)[x]$ gilt. Zum Abzählen der Fixpunkte von π_n benötigen wir folgendes

Lemma 4. *Die Anzahl der Fixpunkte von π_n ist gleich der Anzahl der Elemente $u\in Z/(p^e)$, für welche $((u+\sqrt{\alpha})Z_{p^e})^{n-1}=Z_{p^e}$ gilt.*

Beweis. Sei u Fixpunkt von π_n. Dann gilt $f_n(u)\equiv u \bmod p^e$, also $g_n(u)\equiv u\cdot h_n(u) \bmod p^e$, und somit gilt in $Z(p^e, \alpha)$

$$(u+\sqrt{\alpha})^n = h_n(u)(u+\sqrt{\alpha}).$$

Da $u+\sqrt{\alpha}$ regulär ist, folgt $(u+\sqrt{\alpha})^{n-1}=h_n(u)\in Z_{p^e}$, und daher gilt $((u+\sqrt{\alpha})Z_{p^e})^{n-1}=$ $=Z_{p^e}$.

Sei umgekehrt $((u+\sqrt{\alpha})Z_{p^e})^{n-1}=Z_{p^e}$, also $(u+\sqrt{\alpha})^{n-1}=y\in Z_{p^e}$. Dann gilt $(u+\sqrt{\alpha})^n=yu+y\sqrt{\alpha}=g_n(u)+h_n(u)\sqrt{\alpha}$, und es folgt $g_n(u)\equiv uh_n(u) \bmod p^e$, d.h. $f_n(u)\equiv u \bmod p^e$. Damit ist Lemma 4 bewiesen.

Da die Elemente von U_{p^e}/Z_{p^e} kein Element der Gestalt $\sqrt{\alpha}+u$, die übrigen Elemente von G_{p^e}/Z_{p^e} aber genau ein Element dieser Gestalt enthalten, ist die Anzahl der Fixpunkte von π_n gleich der Anzahl der Lösungen der Gleichung $\xi^{n-1}=1$ in der Gruppe G_{p^e}/Z_{p^e} minus der Anzahl der Lösungen in der Gruppe U_{p^e}/Z_{p^e}. Da $|G_{p^e}/Z_{p^e}|=p^{e-1}(p+1)$, gilt $\xi^{n-1}=1$ in G_{p^e}/Z_{p^e} genau dann, wenn $\xi^{(n-1, p^{e-1}(p+1))}=1$. Die Anzahl der Lösungen dieser Gleichung in der zyklischen Gruppe G_{p^e}/Z_{p^e} beträgt $(n-1, p^{e-1}(p+1))$. Ferner gilt wegen $|U_{p^e}/Z_{p^e}|=p^{e-1}$ in U_{p^e}/Z_{p^e} genau dann $\xi^{n-1}=1$, wenn $\xi^{(n-1, p^{e-1})}=1$; die Anzahl der Lösungen dieser Gleichung in der zyklischen Gruppe U_{p^e}/Z_{p^e} beträgt $(n-1, p^{e-1})$. Wegen $(n-1, p^{e-1}(p+1))=$ $=(n-1, p^{e-1})(n-1, p+1)$ gilt also folgendes

Lemma 5. *Sei $(n, p^{e-1}(p+1))=1$. Dann ist* fix (p^e, n), *die Anzahl der Fixpunkte der durch $f_n(x)$ dargestellten Permutation von $Z/(p^e)$, gegeben durch*

$$\text{fix}\,(p^e, n) = (n-1, p^{e-1})((n-1, p+1)-1).$$

Satz 1. *Sei m eine ungerade natürliche Zahl mit der Primfaktorzerlegung $m=p_1^{e_1}\ldots p_r^{e_r}$, $e_i\geqq 1$, und sei α eine ganze Zahl mit α quadratischer Nichtrest* mod p_i, *$i=1,\ldots,r$. Sei $v=[p_1^{e_1-1}(p_1+1),\ldots,p_r^{e_r-1}(p_r+1)]$, sei n eine natürliche Zahl mit $(n,v)=1$ und sei $d=(n-1,v)$. Dann ist* fix (m,n), *die Anzahl der Fixpunkte der durch $f_n(x)$ dargestellten Permutation von $Z/(m)$, gegeben durch*

$$\operatorname{fix}(m,n)=\prod_{i=1}^{r}(d,p_i^{e_i-1})((d,p_i+1)-1).$$

Beweis. Aus dem Chinesischen Restsatz ergibt sich $\operatorname{fix}(m,n)=\prod_{i=1}^{r}\operatorname{fix}(p_i^{e_i},n)$. Gemäß Lemma 5 gilt $\operatorname{fix}(p_i^{e_i},n)=(n-1,p_i^{e_i-1})((n-1,p_i+1)-1)$. Aus $p_i^{e_i-1}\mid v$ folgt $(n-1,p_i^{e_i-1})=(n-1,v,p_i^{e_i-1})=((n-1,v),p_i^{e_i-1})=(d,p_i^{e_i-1})$, und aus $(p_i+1)\mid v$ folgt $(n-1,p_i+1)=(n-1,v,p_i+1)=((n-1,v),p_i+1)=(d,p_i+1)$. Somit erhält man $\operatorname{fix}(p_i^{e_i},n)=(d,p_i^{e_i-1})((d,p_i+1)-1)$, und daraus ergibt sich die Behauptung.

4. Die Gruppenstruktur. Es seien m, α, v, n und d wie in Satz 1, und es bezeichne π_n die durch $f_n(x)$ induzierte Permutation von $Z/(m)$.

Lemma 6. *Genau dann induziert $f_n(x)$ die Einheitspermutation ε von $Z/(m)$, wenn gilt $n\equiv 1$* mod v.

Beweis. Genau dann gilt $\pi_n=\varepsilon$, wenn jedes Element von $Z/(m)$ Fixpunkt bezüglich π_n ist, und dies ist gleichbedeutend mit $\operatorname{fix}(m,n)=m$. Nach Satz 1 gilt

$$\operatorname{fix}\Big(\prod_{i=1}^{r}p_i^{e_i},n\Big)=\prod_{i=1}^{r}p_i^{e_i}$$

genau dann, wenn gilt $(d,p_i^{e_i-1})=p_i^{e_i-1}$ und $(d,p_i+1)=p_i+1$ für $i=1,\ldots,r$, also dann und nur dann, wenn $p_i^{e_i-1}\mid d$ und $(p_i+1)\mid d$, $i=1,\ldots,r$, und dies ist gleichbedeutend mit $v\mid d$. Da nach Definition von d stest gilt $d\mid v$, ist somit $\pi_n=\varepsilon$ äquivalent zu $v=d$, und damit ist die Behauptung bewiesen.

Lemma 7. *Genau dann induzieren $f_k(x)$ und $f_n(x)$ dieselbe Permutation von $Z/(m)$, wenn gilt $k\equiv n$* mod v.

Beweis. Sei $\pi_k=\pi_n$. Man wähle $l>0$, so, daß $ln\equiv 1$ mod v. Gemäß Lemma 6 gilt

$$\varepsilon=\pi_{ln}=\pi_l\circ\pi_n=\pi_l\circ\pi_k=\pi_{lk}.$$

Aus $\varepsilon=\pi_{lk}$ folgt — wiederum aus Lemma 6 — $lk\equiv 1$ mod v, also $lk\equiv ln$ mod v, und daraus erhält man $k\equiv n$ mod v.

Sei nun andererseits $k\equiv n$ mod v. Wieder wähle man $l>0$ so, daß $ln\equiv 1$ mod v; es gilt dann auch $lk\equiv 1$ mod v. Mit Hilfe von Lemma 6 erhält man

$$\pi_k=\pi_k\circ\pi_{ln}=\pi_k\circ\pi_l\circ\pi_n=\pi_{kl}\circ\pi_n=\pi_n.$$

Satz 2. *Die Gruppe P_m aller jener Permutationen von $Z/(m)$, die durch eine Funktion $f_n(x)$ mit gegebenem α und $(n, v)=1$ induziert werden, ist isomorph zu Z_v, der primen Restklassengruppe von $Z/(v)$.*

Beweis. Nach Lemma 7 ist durch $\psi(\pi_n)=n \bmod v$ eine wohldefinierte und bijektive Abbildung von P_m nach Z_v gegeben. Diese ist wegen (2.3) mit $\circ$ verträglich, also sogar ein Isomorphismus.

Es sollen nun alle ungeraden m ermittelt werden, für die P_m zyklisch ist. Entsprechende Resultate für andere durch Permutationsfunktionen dargestellte Permutationsgruppen findet man z.B. in [2], [5] und in [7].

Satz 3. *Die Gruppe P_m ist genau dann zyklisch, wenn einer der beiden folgenden Fälle vorliegt:*

(a) $m=3$,

(b) $m>3$, *m quadratfrei, und es gibt eine ungerade Primzahl q, sodaß sämtliche Primteiler p_i von m darstellbar sind in der Gestalt*

$$p_i = 2q^{k_i}-1, \quad k_i \geqq 1.$$

Beweis. Nach bekannten Sätzen der Zahlentheorie ist Z_w genau dann zyklisch, wenn w gleich einem der folgenden Werte ist:

(3.1) $$1, 2, 4, q^e, 2q^e \quad (q \text{ ungerade Primzahl}, e \geqq 1).$$

Nach Satz 2 ist P_m isomorph zu $Z_{v(m)}$. Wir haben also alle ungeraden natürlichen Zahlen $m \geqq 3$ zu bestimmen, für die $v(m)$ einen der Werte (3.1) annimmt. (Da es keine quadratischen Nichtreste modulo 1 gibt, existiert P_1 nicht.)

Es gilt für alle ungeraden m mit $m \geqq 3$, daß $v(m) \geqq 4$, also nimmt $v(m)$ für kein in Frage kommendes m die Werte 1 oder 2 an. Weiters gilt $v(m)=4$ genau dann, wenn $m=3$.

Sei im folgenden q eine feste ungerade Primzahl, und sei $e \geqq 1$.

Angenommen, es gibt ein ungerades $m \geqq 3$ mit $v(m)=q^e$. Sei p_i ein Primteiler von m, dann gilt $(p_i+1) | v(m)$, also $(p_i+1) | q^e$. Daraus folgt $2 | q^e$, und dies ergibt einen Widerspruch. Es gibt also keine ungeraden Zahlen m mit $v(m)=q^e$.

Sei nun $m \geqq 3$ eine ungerade Zahl mit $v(m)=2q^e$. Sei p_i ein Primteiler von m, und sei $v_{p_i}(m)$ die Vielfachheit, mit der p_i in der Faktorzerlegung von m vorkommt. Wäre $v_{p_i}(m)>1$, dann gälte $p_i(p_i+1) | v(m)$, also $p_i(p_i+1) | 2q^e$, und dies ergäbe einen Widerspruch zu p_i ungerade. Also gilt $v_{p_i}(m)=1$. Wegen $(p_i+1) | v(m)$ gilt $(p_i+1) | 2q^e$, und daraus folgt $p_i+1=2q^s$ mit $1 \leqq s \leqq e$, also $p_i=2q^s-1$. Die Zahl m ist also von der Gestalt (b).

Sei andererseits m von der Gestalt (b), und sei r die Anzahl der Primfaktoren von m. Dann gilt

$$v(m) = [2q^{k_1}, \ldots, 2q^{k_r}] = 2q^{\max\{k_1, \ldots k_r\}},$$

d.h. $v(m)$ ist von der Gestalt $2q^e$, und P_m ist zyklisch. Damit ist Satz 3 vollständig bewiesen.

Als unmittelbare Folgerung erhält man: Mit Ausnahme von 3 gibt es keine natürlichen Zahlen m mit $m \equiv 3 \bmod 4$, für die P_m zyklisch ist.

5. Eigenschaften der Fixpunktanzahl. Es sollen nun einige mit der Fixpunktanzahl fix (m, n) in Zusammenhang stehende Fragen erörtert werden. Wie Satz 1 zeigt, ist fix (m, n) bei gegebenem m durch d eindeutig bestimmt. Bezeichnet man für einen festen Teiler d von v die Anzahl der Permutationen $\pi_n \in P_m$, für die gilt $(n-1, v)=d$, mit $\sigma(d, v)$, dann gilt

Satz 4. *Sind* $v=\prod_{j=1}^{s} q_j^{g_j}$, $g_j \geqq 1$, *und* $d=\prod_{j=1}^{s} q_j^{h_j}$, $0 \leqq h_j \leqq g_j$, *die Primfaktorzerlegungen der Zahlen v und d, so gilt*

$$\sigma(d, v) = (v/d) \prod_{j=1}^{s} (1-\varepsilon_j/q_j) \quad \text{mit} \quad \varepsilon_j = \begin{cases} 2 & \text{für } h_j = 0, \\ 1 & \text{für } 0 < h_j < g_j, \\ 0 & \text{für } h_j = g_j. \end{cases}$$

Beweis. (Vgl. [4], wo ein analoges Resultat für die Gruppe der durch die Potenzen x^n induzierten Permutationen von $Z/(m)$ hergeleitet wird.) Klarerweise ist $\sigma(d, v)$ die Anzahl der Restklassen a mod v mit $(a, v)=d$ und $(a+1, v)=1$. Nach dem Chinesischen Restsatz kann man die Restklassen a mod v bijektiv zuordnen den s-Tupeln $(a_1, \ldots, a_s)$, in denen a_j jeweils alle Restklassen modulo $q_j^{g_j}$ durchläuft. Mit Hilfe der Gleichungen $a=a_j+k_j q_j^{g_j}$, $j=1, \ldots, s$, erkennt man

$$(a, v) = \prod_{j=1}^{s} (a, q_j^{g_j}) = \prod_{j=1}^{s} (a_j+k_j q_j^{g_j}, q_j^{g_j}) = \prod_{j=1}^{s} (a_j, q_j^{g_j}).$$

Da der Restklasse $a+1$ das s-Tupel $(a_1+1, \ldots, a_s+1)$ entspricht, ist $(a+1, v)=1$ gleichbedeutend mit $(a_j+1, q_j^{g_j})=1$ für alle j und dies wiederum ist gleichbedeutend mit $a_j \not\equiv -1 \bmod q_j$, $j=1, \ldots, s$. Ferner ist $(a_j, q_j^{g_j})=q_j^{h_j}$ gleichbedeutend damit, daß $a_j=bq_j^{h_j}$ mit $(b, q_j)=1$. Die Anzahl der verschiedenen Restklassen a_j mod $q_j^{g_j}$, die diese und die vorhergehende Bedingung erfüllen, ist also gegeben durch

$$q_j^{g_j-h_j-1}(q_j-\varepsilon_j) = q_j^{g_j-h_j}(1-\varepsilon_j/q_j),$$

woraus die Behauptung folgt.

Lemma 8. *Sei d ein Teiler von v. Es gilt* $\sigma(d, v)=0$ *genau dann, wenn d ungerade ist.*

Beweis. Da m ungerade ist, hat m einen ungeraden Primteiler p_i, und es folgt $(p_i+1) \mid v$, also $2 \mid v$. Sei o.B.d.A. $q_1=2$. Aufgrund von Satz 4 gilt $\sigma(d, v)=0$ genau dann, wenn für ein $j \in \{1, \ldots, s\}$ gilt $1-\varepsilon_j/q_j=0$, d.h. wenn für ein j gilt $\varepsilon_j=q_j$.

Wegen $\varepsilon_j \leqq 2 \leqq q_j$ gilt dies höchstens für $q_j=2$, also für $j=1$. Es gilt $\varepsilon_1=q_1$, also $\varepsilon_1=2$ genau dann, wenn $h_1=0$, also wenn d ungerade ist. Damit ist das Lemma bewiesen.

Für kryptographische Anwendungen sind speziell die beiden folgenden Problemstellungen von Interesse: (i) Welches ist die kleinste Zahl $w_{\min}$, die als Fixpunktanzahl einer Permutation $\pi_n \in P_m$ auftreten kann? (ii) Wieviele Permutationen $\pi_n \in P_m$ gibt es, die genau $w_{\min}$ Fixpunkte aufweisen?

Aufgrund von Satz 1 und Lemma 8 treten als Fixpunktanzahlen von Permutationen $\pi_n \in P_m$ genau die Zahlen

$$\tau(d, m) = \prod_{i=1}^{r} (d, p_i^{e_i-1})((d, p_i+1)-1), \quad d \text{ gerader Teiler von } v$$

auf. Setzt man $d=2$, so erhält man $\tau(2, m)=1$. Es gibt also Permutationen $\pi_n \in P_m$ mit nur einem Fixpunkt. Um die Anzahl aller $\pi_n \in P_m$ mit nur einem Fixpunkt bestimmen zu können, benötigt man

Satz 5. *Die Funktion $\tau(d, m)$ ist streng monoton auf dem Verband der geraden Teiler von v.*

Beweis. Es ist zu zeigen, daß $\tau(c, m) < \tau(d, m)$, wenn c ein echter Teiler von d ist. Da dann $(c, p_i^{e_i-1}) | (d, p_i^{e_i-1})$ und $(c, p_i+1) | (d, p_i+1)$ für alle i, also $(c, p_i^{e_i-1}) \leqq (d, p_i^{e_i-1})$ und $(c, p_i+1) \leqq (d, p_i+1)$, folgt jedenfalls $\tau(c, v) \leqq \tau(d, v)$. Sei q_j eine Primzahl, die in c mit der Vielfachheit $v_{q_j}(c)$ und in d mit der Vielfachheit $v_{q_j}(d) > v_{q_j}(c)$ vorkommt. Wegen $d | v$ gilt $v_{q_j}(d) \leqq v_{q_j}(v) = \max\limits_{1 \leqq i \leqq r} \{v_{q_j}(p_i^{e_i-1}(p_i+1))\}$. Also gibt es ein i mit $q_j^{v_{q_j}(d)} | p_i^{e_i-1}(p_i+1)$. Ist $q_j=p_i$, dann gilt $(c, p_i^{e_i-1}) < (d, p_i^{e_i-1})$. Ist aber $q_j \neq p_i$, dann gilt $(c, p_i+1) < (d, p_i+1)$. Daher gilt jedenfalls $(c, p_i^{e_i-1})((c, p_i+1)-1) < (d, p_i^{e_i-1})((d, p_i+1)-1)$, und daraus folgt $\tau(c, m) < \tau(d, m)$.

Folgerung 1. *Die Anzahl der Permutationen $\pi_n \in P_m$ mit nur einem Fixpunkt beträgt*

$$(v/2\delta) \prod_{j=2}^{s} (1-2/q_j) \quad \text{mit} \quad \delta = \begin{cases} 1 & \text{für } v \not\equiv 0 \bmod 4 \\ 2 & \text{für } v \equiv 0 \bmod 4. \end{cases}$$

Beweis. Sei d ein gerader, von 2 verschiedener Teiler von v. Dann ist 2 echter Teiler von d, und aus Satz 5 folgt $1=\tau(2, m) < \tau(d, m)$. Somit ist die Anzahl der Permutationen π_n von $Z/(m)$ mit nur einem Fixpunkt gleich $\sigma(2, v)$. Aufgrund von Satz 4 folgt daraus unmittelbar die Behauptung.

6. Kryptographische Anwendung. Es soll nun die Beschreibung eines Public-Key Kryptosystems auf der Basis der Rédei-Funktionen erfolgen.

Jeder potentielle Kommunikationsteilnehmer C wählt eine Faktorenanzahl r und r große Primfaktoren $p_1, \ldots, p_r$ mit zugehörigen Vielfachheiten $e_1, \ldots, e_r$, bildet das Produkt $m = \prod_{i=1}^{r} p_i^{e_i}$ und berechnet die gemäß Satz 1 definierte Größe v. Weiters wählt C eine ganze Zahl α mit α Nichtrest mod p_i, $i=1, \ldots, r$ — etwa durch sukzessives Testen zufällig gewählter Testzahlen a mit Hilfe des Eulerschen Kriteriums. Schließlich wählt C einen Chiffrierschlüssel $n>0$ mit

$$(n, v) = 1 \tag{6.1}$$

und

$$(n-1, v) = 2 \tag{6.2}$$

und berechnet zu diesem n durch Lösen der linearen Kongruenz

$$nk \equiv 1 \bmod v \tag{6.3}$$

einen zugehörigen Dechiffrierschlüssel $k>0$. Im öffentlich zugänglichen Schlüsselverzeichnis veröffentlicht C die Größen $m_C=m$, $\alpha_C=\alpha$ und $n_C=n$, hält jedoch die Faktorzerlegung von m sowie $k_C=k$ und $v_C=v$ geheim.

Angenommen, A möchte an B die Nachricht φ übersenden. A sucht aus dem öffentlich zugänglichen Schlüsselverzeichnis die Schlüsselparameter von B, also m_B, α_B und n_B, stellt die Nachricht φ als Folge von Blöcken x_i, $x_i \in Z/(m_B)$, dar, chiffriert die x_i mittels

$$x_i \to y_i = f_{n_B}(x_i) \bmod m_B \tag{6.4}$$

und übersendet die y_i an B. Der Empfänger berechnet mit Hilfe des nur ihm bekannten Dechiffrierexponenten k_B aus den y_i die Nachrichtenblöcke x_i:

$$f_{k_B}(y_i) = f_{k_B} \circ f_{n_B}(x_i) = f_{k_B n_B}(x_i) = f_{1+tv_B}(x_i) \equiv x_i \bmod m_B.$$

Dabei steht t für eine geeignete natürliche Zahl, und die letzte Gleichung gilt aufgrund von Lemma 6.

Da zur Berechnung von v_B die Faktorzerlegung von m_B benötigt wird, jedoch bis heute keine schnellen Algorithmen zur Faktorisierung großer Zahlen bekannt sind, ist es nicht möglich, aufgrund der öffentlich bekannten Informationen m_B, α_B und n_B das zur Berechnung des Dechiffrierschlüssels k_B benötigte v_B zu ermitteln. Forderung (6.2) garantiert, daß die durch $f_n(x)$ induzierte Chiffrierfunktion nur *einen* Fixpunkt aufweist.

Literatur

[1] W. Diffie und M. Hellman, New directions in cryptography, *IEEE Trans. Information Theory*, IT—22 (1976), 644—654.

[2] H. Hule und W. B. Müller, Grupos cíclicos de permutaciones inducidas por polinomios sobre campos de Galois, *An. Acad. Brasil. Cienc.*, 45 (1973), 63—67.

[3] R. Lidl und W. B. Müller, Permutation polynomials in RSA-cryptosystems, in: *Proceedings Crypto 83*, University California, Santa Barbara, 1983.

[4] W. B. Müller und W. Nöbauer, Über die Fixpunkte der Potenzpermutationen, *Österr. Akad. Wiss. Math. Naturwiss. Kl. Sitzungsber.*, II (1983), 93—97.

[5] W. Nöbauer, Über eine Gruppe der Zahlentheorie, *Monatsh. Math.*, 58 (1954), 181—192.

[6] W. Nöbauer, Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen, *Monatsh. Math.*, 69 (1965), 230—238.

[7] W. Nöbauer, Über Gruppen von Dickson-Polynomfunktionen und einige damit zusammenhängende zahlentheoretische Fragen, *Monatsh. Math.*, 77 (1973), 330—344.

[8] L. Rédei, Über eindeutig umkehrbare Polynome in endlichen Körpern, *Acta Sci. Math.*, 11 (1946), 85—92.

[9] R. Rivest, A. Shamir und L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, 21 (1978), 120—126.

UBW KLAGENFURT
UNIVERSITÄTSSTRASSE 67
9010 KLAGENFURT, AUSTRIA